

Exhibit 8

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1pre] A method of establishing plural modes of operation on a mobile device, the method comprising:</p>	<p>Sophos Mobile is an endpoint (e.g., mobile device) management tool</p>  <p>Why Sophos Mobile?</p> <p>Sophos Mobile is a secure Unified Endpoint Management (UEM) solution that helps businesses spend less time and effort to manage and secure traditional and mobile endpoints. The only UEM solution that integrates natively with a leading next-gen endpoint security platform, Sophos Mobile supports management of Windows 10, macOS, iOS, and Android devices.</p> <ul style="list-style-type: none"> Productivity Let mobile users work the way they want, on whatever devices they want — securely. Security Ensure business data doesn't go adrift and isn't threatened by malware. Simplicity Easy to configure, manage, and maintain. Value User-based pricing lets you manage and secure endpoints affordably. <p>Sophos Mobile Secure Unified Endpoint Management</p> <p>EXPERTS AGREE Sophos is a leader in secure device management</p> <p>https://www.sophos.com/en-us/products/mobile-control</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Sophos Mobile supports BYOD environments through the management “mode” of Android (Android Enterprise Work Profile) to separate business and personal data. For example, corporate email and apps remain separate from personal data. It is possible to configure “policies” and establish “blacklist” and “whitelist” applications.</p> <div data-bbox="625 502 1786 1019">  <p>Sophos Mobile Means Enterprise Mobility Management Manage in Sophos Central</p> <p>Devices</p> <ul style="list-style-type: none"> ✓ iOS, Android, Windows 10, macOS ✓ Configuration and policies ✓ Inventory and asset management ✓ Detailed reporting <p>Apps</p> <ul style="list-style-type: none"> ✓ Install, remove, and view apps ✓ Enterprise app store ✓ App control, whitelist/blacklist ✓ Manage and configure Office 365 apps <p>Flexible</p> <ul style="list-style-type: none"> ✓ Manage corporate devices ✓ Manage bring-your-own-device (BYOD) ✓ Secure business data ✓ Respect user privacy <p>Security</p> <ul style="list-style-type: none"> ✓ Extended Detection and Response ✓ Malware, ransomware, PUAs ✓ Anti-phishing ✓ Web protection, web filtering <p>Bring Your Own Device? No Problem!</p> <p>Sophos Mobile lets you secure any combination of personal and corporate-owned devices with minimal effort.</p> <p>Sophos Mobile supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrollment modes of management to ensure that business data is safe and personal information is private. Deploy corporate email and apps to a device and feel safe knowing these remain separate from a user's personal data, enabling productivity without compromising security.</p> </div> <p>https://www.sophos.com/en-us/products/mobile-control</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1a] associating each application on the mobile device with one of a plurality of modes; and	<p>Sophos Mobile supports the use of Android Enterprise Work Profile mode.</p> <div data-bbox="671 465 1875 975" style="border: 1px solid black; padding: 10px;"><p>Bring Your Own Device? No Problem!</p><p>Sophos Mobile lets you secure any combination of personal and corporate-owned devices with minimal effort.</p><p>Sophos Mobile supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrollment modes of management to ensure that business data is safe and personal information is private. Deploy corporate email and apps to a device and feel safe knowing these remain separate from a user's personal data, enabling productivity without compromising security.</p></div>

<https://www.sophos.com/en-us/products/mobile-control>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Sophos Mobile supports the use of Android Enterprise Work Profile mode.</p> <div data-bbox="739 399 1784 1101"><h2>Get started with work profile management</h2><p>Apr 3, 2024</p><p>This page shows you how to set up the Android Enterprise work profile management mode and enroll personal devices.</p><p>The work profile management mode lets you manage a dedicated workspace, the work profile, on a user's Android device. This management mode is commonly used for a bring your own device (BYOD) setup, because you can only monitor and manage apps, accounts, and data within the work profile.</p><p>Requirements</p><ul style="list-style-type: none">You set up Android Enterprise in Sophos Mobile. See Set up Android Enterprise.You added the device user to Sophos Central. See Users.You created the device group you want to add the device to. See Device groups.<p>See the following sections to learn how to set up Android Enterprise work profile enrollment and enroll devices.</p></div> <p>https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Sophos Mobile supports the use of Android Enterprise Work Profile mode, which separates “work” and “personal” apps and data.</p> <p>https://www.android.com/enterprise/work-profile/</p>

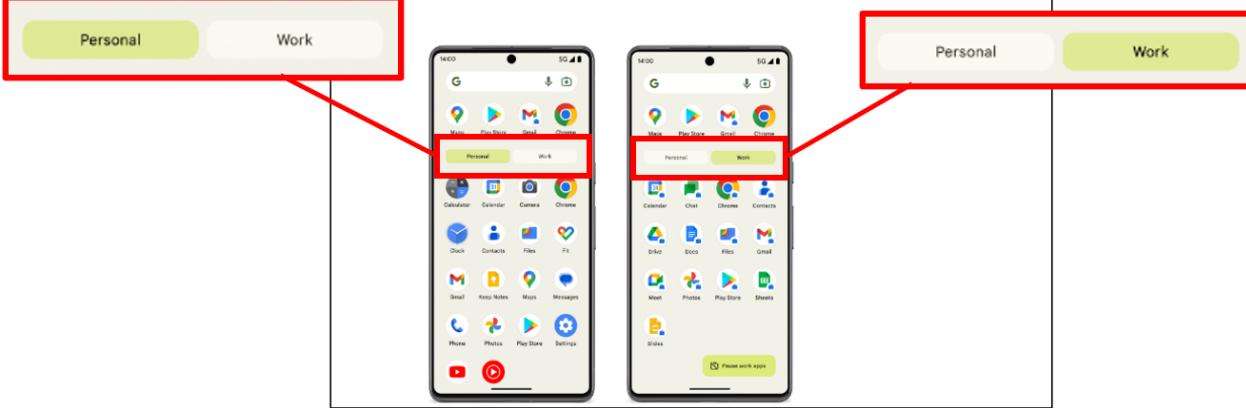
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div style="border: 2px solid red; padding: 10px;"><p>Work Profile and its features</p><p>A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device’s personal profile and overall device behavior.</p><p>Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile.</p></div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification										
	<p>In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div data-bbox="713 474 1769 1041" style="border: 1px solid black; padding: 10px;"><p>App management</p><p>EMM providers support Android app management through an enterprise version of Google Play, called managed Google Play. With an EMM, you can create Managed Google Play accounts* for your users. These accounts enable app distribution to their Work Profiles.</p><table border="1" data-bbox="722 659 1727 951"><thead><tr><th data-bbox="722 659 1056 698">Feature</th><th data-bbox="1056 659 1727 698">Description</th></tr></thead><tbody><tr><td data-bbox="722 698 1056 780">View and manage your app catalog</td><td data-bbox="1056 698 1727 780">View a list of purchased apps, approved apps, and private apps.</td></tr><tr><td data-bbox="722 780 1056 829">Distribute apps silently</td><td data-bbox="1056 780 1727 829">Silently install apps on a device without any user interaction.</td></tr><tr><td data-bbox="722 829 1056 910">Download apps from the managed Play app</td><td data-bbox="1056 829 1727 910">Users can install and update apps approved for them through the Managed Google Play app on their device.</td></tr><tr><td data-bbox="722 910 1056 951">Set managed configurations</td><td data-bbox="1056 910 1727 951">Configure work apps for individual users or devices.</td></tr></tbody></table><p>*For organizations with Google Workspace or Cloud Identity, users can access managed Google Play with their Google Workspace or Cloud Identity account.</p></div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	View and manage your app catalog	View a list of purchased apps, approved apps, and private apps.	Distribute apps silently	Silently install apps on a device without any user interaction.	Download apps from the managed Play app	Users can install and update apps approved for them through the Managed Google Play app on their device.	Set managed configurations	Configure work apps for individual users or devices.
Feature	Description										
View and manage your app catalog	View a list of purchased apps, approved apps, and private apps.										
Distribute apps silently	Silently install apps on a device without any user interaction.										
Download apps from the managed Play app	Users can install and update apps approved for them through the Managed Google Play app on their device.										
Set managed configurations	Configure work apps for individual users or devices.										

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div style="border: 1px solid black; padding: 10px;"> <p>What is an Android Work Profile?</p> <p><i>Android 5 or later devices only</i></p> <p>An Android Work Profile can be set up on an Android device to separate work apps and data from personal apps and data. With a Work Profile you can securely and privately use the same device for work and personal purposes—your organization manages your work apps and data while your personal apps, data, and usage remain private.</p> <p>Note: Work Profile apps can't access SMS/MMS data from the personal profile on Android 11+.</p> <p>If your organization supports enrolling devices to use a Work Profile, your IT department should provide instructions on how to add one to your device.</p>  </div> <p>https://support.google.com/work/android/answer/6191949?hl=en</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
[1b] restricting data on the mobile device to be accessible by only a subset of applications based on the mode associated with the application,	<p>Android Enterprise Work Profile enables the creation of “approved app lists” that restricts data accessed by applications based on the mode.</p> <div data-bbox="684 528 1867 926"><h2>Highlights</h2><ul style="list-style-type: none">✓ Unlock personal devices Allow employees to use personal Android devices for work with full management control over data in Work Profile only.✓ Manage approved app lists Choose which apps your employees can access on the Work Profile without restricting apps they can access on their personal profile.✓ Remotely provision devices Provision company-owned devices remotely with zero-touch enrollment and get employees up-and-running right out of the box.</div> <p>https://www.android.com/enterprise/work-profile/</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile restricts data to be accessible based on the mode associated with the app, as apps are restricted to segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles.</p> <div data-bbox="713 507 1818 1106" style="border: 2px solid red; padding: 10px;"><p>Data segregation</p><p>Work profiles use the following data segregation rules.</p><p>Apps 🔗</p><p>When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold INTERACT_ACROSS_PROFILES permission or App-ops.</p><p>Accounts</p><p>Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p><p>Intents</p><p>The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</p></div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <p>What policies is my organization enforcing on my device?</p> <p>If your device has a work profile, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren’t visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned.</p> <p>https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <div data-bbox="654 620 1795 816" style="border: 2px solid red; padding: 10px;"><p>Work profile More Send feedback</p><p>The work profile solution set is intended for employee-owned devices and company-owned devices for work and personal use. Corporate apps, data, and management policies are restricted to the work profile. With a work profile, the same device can be used securely and privately for work and personal purposes.</p></div> <p>https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app. Sophos Mobile provides a device policy controller app for implementing and managing Android Enterprise Work Profile.</p> <div data-bbox="804 421 1628 997" style="border: 2px solid red; padding: 10px;"><p>What policies can my organization manage on my device?</p><p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p><p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p><ul style="list-style-type: none">• Remotely create, access, and delete data in your work profile• Enforce minimum passcode requirements on your work profile and device• Change the password to your managed account (the account associated with your work profile)• Suspend access to your work profile• Restrict what can be shared across your work and personal profiles• Block screen captures in your work profile• Manage access to your organization's corporate mail server and internal data• Remotely install (and uninstall) apps and certificates in your work profile• Manage permissions and other settings for apps in your work profile</div> <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p>Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <div data-bbox="741 442 1733 1090" style="border: 1px solid black; padding: 10px;"> <p>Device management</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th data-bbox="783 518 1079 540">Feature</th><th data-bbox="1079 518 1691 540">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="783 561 1079 616">Manage Google Workspace accounts</td><td data-bbox="1079 561 1691 616">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="783 638 1079 709">Manage 3rd party certificates</td><td data-bbox="1079 638 1691 709">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="783 731 1079 786">Control access to input methods</td><td data-bbox="1079 731 1691 786">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.</td></tr> <tr> <td data-bbox="783 824 1079 879">Control access to accessibility services</td><td data-bbox="1079 824 1691 879">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="783 900 1079 956">Set location sharing preferences</td><td data-bbox="1079 900 1691 956">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="783 979 1079 1018">Disable screen captures</td><td data-bbox="1079 979 1691 1018">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="783 1039 1079 1078">Retrieve network statistics</td><td data-bbox="1079 1039 1691 1078">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> </div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1c] wherein the data is associated with one of the plurality of modes and the restricting comprises adding a group permission to the data and providing each application with access to the data based on the group permission, the group permission for data associated with one of the plurality of modes controls access to the data by applications associated with the others of the plurality of modes, and</p>	<p>Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div style="border: 2px solid red; padding: 10px;"> <p>Data segregation</p> <p>Work profiles use the following data segregation rules.</p> <p>Apps ➔</p> <p>When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold <code>INTERACT_ACROSS_PROFILES</code> permission or App-ops.</p> <p>Accounts</p> <p>Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p> <p>Intents</p> <p>The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</p> </div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="713 584 1799 889" style="border: 2px solid red; padding: 10px;"><p>What policies is my organization enforcing on my device?</p><p>If your device has a work profile, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned.</p></div> <p>https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="650 665 1797 850" style="border: 2px solid red; padding: 10px;"><p>Work profile □ ▾ Send feedback</p><p>The work profile solution set is intended for employee-owned devices and company-owned devices for work and personal use. Corporate apps, data, and management policies are restricted to the work profile. With a work profile, the same device can be used securely and privately for work and personal purposes.</p></div> <p>https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div style="border: 2px solid red; padding: 10px;"> <p>What policies can my organization manage on my device?</p> <p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • <u>Restrict what can be shared across your work and personal profiles</u> • Block screen captures in your work profile • <u>Manage access to your organization's corporate mail server and internal data</u> • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p>Android Enterprise Work Profile segregates data and associates data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="747 528 1727 1165" style="border: 1px solid black; padding: 10px;"> <p>Device management</p> <table border="1" data-bbox="789 594 1698 1148"> <thead> <tr> <th data-bbox="789 594 1064 626">Feature</th><th data-bbox="1064 594 1698 626">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="789 626 1064 708">Manage Google Workspace accounts</td><td data-bbox="1064 626 1698 708">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="789 708 1064 789">Manage 3rd party certificates</td><td data-bbox="1064 708 1698 789">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="789 789 1064 904">Control access to input methods</td><td data-bbox="1064 789 1698 904">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.</td></tr> <tr> <td data-bbox="789 904 1064 969">Control access to accessibility services</td><td data-bbox="1064 904 1698 969">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="789 969 1064 1034">Set location sharing preferences</td><td data-bbox="1064 969 1698 1034">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="789 1034 1064 1099">Disable screen captures</td><td data-bbox="1064 1034 1698 1099">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="789 1099 1064 1148">Retrieve network statistics</td><td data-bbox="1064 1099 1698 1148">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> </div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1d] the group permission for the data limits the ability to copy a subset of the data between modes, where some data can be copied directly between modes, and</p>	<p>Android Enterprise Work Profile policies can limit the ability to copy data between modes.</p> <div style="border: 1px solid black; padding: 10px;"> <p>What policies can my organization manage on my device?</p> <p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p>Android Enterprise Work Profile policies can limit the ability to copy data between modes.</p> <table border="1" data-bbox="747 442 1740 1090"> <caption>Device management</caption> <thead> <tr> <th data-bbox="789 512 1043 545">Feature</th><th data-bbox="1043 512 1698 545">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="789 561 1043 610">Manage Google Workspace accounts</td><td data-bbox="1043 561 1698 610">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="789 626 1043 675">Manage 3rd party certificates</td><td data-bbox="1043 626 1698 708">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="789 724 1043 773">Control access to input methods</td><td data-bbox="1043 724 1698 806">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.</td></tr> <tr> <td data-bbox="789 822 1043 871">Control access to accessibility services</td><td data-bbox="1043 822 1698 871">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="789 887 1043 936">Set location sharing preferences</td><td data-bbox="1043 887 1698 936">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="789 953 1043 1002">Disable screen captures</td><td data-bbox="1043 953 1698 1002">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="789 1018 1043 1051">Retrieve network statistics</td><td data-bbox="1043 1018 1698 1051">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles.																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1e] wherein data associated with the first mode is deleted from the mobile device when such data is not accessed within a time period, while data associated with the second mode does not have a deletion policy.</p>	<p>Android Enterprise Work Profile allows work profile administrator to control the “lifetime” and “egress” of data.</p> <div data-bbox="768 540 1797 1008" style="border: 1px solid black; padding: 10px;"> <h2>Employing Work Profiles</h2> <p>A <i>work profile</i> is a <i>managed profile</i> that has separate app data from the primary user profile but shares some system-wide settings, such as Wi-Fi and Bluetooth. The primary goal of a work profile is to create a segregated and secure container to hold managed data. <u>The administrator of a work profile has full control over the scope, ingress, egress, and lifetime of data.</u> Following are some characteristics of work profiles:</p> <ul style="list-style-type: none"> • Creation. Any app in the primary user can create a work profile. The user is notified of work profile behaviors and policy enforcement before creation. • Management. Apps known as <i>profile owners</i> can programmatically invoke APIs in the <code>DevicePolicyManager</code> class to restrict use. Profile owners are defined at initial profile setup. Policies unique to work profiles involve app restrictions, updatability, and intent behaviors. • Visual treatment. Apps, notifications, and widgets from the work profile are badged and typically made available inline with user interface (UI) elements from the primary user. </div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile allows work profile administrator to control the deletion of data.</p> <p>What policies can my organization manage on my device?</p> <p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul style="list-style-type: none">• Remotely create, access, and <u>delete</u> data in your work profile• Enforce minimum passcode requirements on your work profile and device• Change the password to your managed account (the account associated with your work profile)• Suspend access to your work profile• Restrict what can be shared across your work and personal profiles• Block screen captures in your work profile• Manage access to your organization's corporate mail server and internal data• Remotely install (and uninstall) apps and certificates in your work profile• Manage permissions and other settings for apps in your work profile <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>